Paper

A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence

Marek Janiszewski, Anna Felkner, and Piotr Lewandowski

Information Security Methods Team, Research and Academic Computer Network (NASK), Warsaw, Poland

https://doi.org/10.26636/jtit.2019.130919

Abstract—Real-time assessment of IT-related risks, performed at the national level, is very important due to the evolving nature of threats that may originate from individual hackers, organized cyber-criminal groups, as well as state activities. Evaluation of risk that is based on technical information, as well as on mutual relationships between various institutions and services, may result in very valuable situational awareness. The paper describes (in general) cyber risk analysis method which will be implemented in Polish National Cybersecurity Platform.

Keywords*—*digital services, essential services, incident management, risk assessment, risk management, situational awareness, threat intelligence, vulnerability management.

1. Introduction

The main goal of the National Cybersecurity Platform is to provide a comprehensive, state-wide view of cyber threats in order to evaluate risks in real-time, as well as to monitor the current status of various essential, digital services. In cybersecurity, the broader the perspective, the more threats may be noticed. Therefore, various relationships may be identified to prevent many ramifications, helping protect the essential services, their operators and, as a consequence, various entities and citizens. The National Cybersecurity Platform consists of two types of entities, namely the platform's customers and its operational center. Any institution may become a customer of the platform, but essential service operators and digital service providers may be obliged to become its members. The operational center is a central unit that provides customers with various types of information and acts as an intermediary in sharing information between individual users. The operational center monitors also various events, calculates risks based on the information provided by customers, submits information on current threat levels and provides recommendations based on the risk analyses performed.

Risk estimation relying on objective and quantified measures is very rare, due to the fact that it is a non trivial task. Most solutions use qualified measures to assess the risk affecting information systems that use different programs. Risk estimation is based on a methodology that tries to ensure objective nature of the risk assessment process. However, such an approach requires that the task be always performed by an analyst or auditor (with the support of a specific methodology and a system that may facilitate this process). Due to the fact that the human factor is involved, the results of such a risk assessment process are, to some extent, always subjective. In addition, this process is time-consuming and is repeated not more frequently than once every few months (in most cases risk assessment is performed annually or every other year). The fact that such analysis often fails to focus on technical vulnerabilities of software and on and other technical information (such as Indicators of Compromise – IoC) also needs to be taken into account. In fact, such technical information plays a key role in assessing the level of security of a given system or service. In addition, new vulnerabilities are still being discovered (with new incidents and IoCs being reported as well). Therefore, risk estimation should be carried out in real-time [1]. The statements given above are true even for individual institutions, but at a higher level (for example – within a given economic sector) the task of risk assessment is significantly more complicated. On the national level, due to the heterogeneity of institutions (and sectors), the task is much more difficult, but this paper presents a general approach which may be relied upon to satisfy the need of quantitative risk assessment performed on the national level.

The article is organized as follows. Section 2 discusses works related to the risk analysis domain. Section 3 describes, in more detail, the main characteristics of the approach used to model relationships between services and also the general approach to risk calculation. Section 4 lists and describes the sources of information which are used to calculate risk and monitor situational awareness. Section 5 presents the model of the proposed risk calculation algorithm. Conclusions and proposals of future work are provided in Section 6.

2. State of the Art

Risk management is very important, but no comprehensive frameworks exist facilitating the performance of this task on the national level. In most cases the problem is considered with regard to an individual institution, and cannot be easily transposed to the national level. Still, approaches exist which may be relied upon in a more comprehensive manner. Therefore, this section briefly describes the most important problems and approaches associated to risk assessment.

2.1. Standards and Norms

The best-known risk management methods and methodologies include the following:

- ISO 16085:2006 – Systems and software engineering – Life cycle processes – Risk management,
- ISO 31000 Risk management – Principles and guidelines,
- ISO/IEC 27005:2014,
- AS/NZS 4360:2004 – Risk Management,
- COSO Enterprise Risk Management,
- FERMA Risk Management Standard,
- CRAMM – CCTA Risk Analysis and Management Method,
- COBRA – Control Objectives for Risk Analysis,
- OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation,
- MARION – Methodology of Analysis of Computer Risks Directed by Levels,
- MEHARI – MEthod for Harmonized Analysis of RIsk.

All standards and methods referred to above are very useful in the context of risk management at the level of individual organizations. Guidelines contained in the above standards may be applied within an institution, whereas in order to estimate the risk on the level of the entire cyberspace, where no access to information about the infrastructure of individual institutions is available, such guidelines prove to be insufficient. They may be taken into account, but unfortunately, they cannot be applied directly.

2.2. Types of Tools Relevant for Risk Assessment

Risk assessment, risk analysis and risk management processes of an organization may be supported with different types of software, covering various domains. The most comprehensive tool for this work is a GRC system (Governance, Risk management, and Compliance). Applications such as IBM OpenPages (for more details, see IBM website [2]) may help to define risks, connect them with the organization's missions, assets and responsible people, as well as rate and manage these risks. This approach is very much focused on the business dimension, so it lacks some detailed technical information required by those who are more interested in analyzing risks affecting IT assets and resources.

To overcome those shortcomings of GRC software, some ITAM (IT Asset Management) and Configuration Management Database (CMDB) applications have been designed, incorporating IT inventory risk analysis modules. ITAM software (e.g. Device42 [3]) helps manage the IT asset life-cycle in an organization (i.e. cost, warranty, ownership, depreciation), while CMDB (e.g. BMC Discovery [4] or Qualys Asset Inventory [5]) applications store the configuration of IT assets (both hardware and software) and their current operational status. In spite of differences in core functionality of ITAM and CMDB applications, both store some information about the configuration of IT assets. Combining this data with information about well-known vulnerabilities may help performing in risk analysis and management processes.

Complex platforms composed of modules (such as ITAM, CMDB, GRC etc.) which cooperate to cover every aspect of risk assessment, analysis and management are also available. These include, for instance: RSA Archer and ServiceNow Now Platform. Even if the manufacturer is not offering its own module for a certain task, the platform can import data from a third party application via API. A detailed description of these platforms may be found on their respective websites: [6], [7].

2.3. International Projects

While conducting research, we analyzed several international, EU-funded projects concerning IT security and risk analysis. The most important of these include the following: PANOPTESEC, WISER, PROTECTIVE and NECOMA. Some of them (NECOMA or PANOPTESEC) focus, to a more considerable degree, on IT security, while others (WISER, PROTECTIVE) attach a greater emphasis to risk analysis. In the following subsections, the authors' conclusions about these projects, which are important in the context of the objectives of the article, may be found.

The NECOMA project [8] was driven by European and Japanese organizations: Institut Mines-Télécom (France), Atos Spain (Spain), 6cure (France), NASK – Research and Academic Computer Network (Poland), Foundation for Research and Technology – Hellas (Greece), Nara Institute of Science and Technology (Japan), Internet Initiative Japan Inc. (Japan), National Institute of Informatics (Japan), Keio University (Japan) and University of Tokyo (Japan). The main goal of the NECOMA project was to create a tool for collecting network traffic, analyzing it, identifying cyber-attack attempts and mitigating them. The idea was to collect data from network devices, such as switches, routers, IDS, etc., and to analyze such data in a dedicated system with the use of original algorithms. This system also uses external databases, such as n6 [9] or PhishTank [10], to improve the ability to detect attacks [11]. In order to mitigate attacks, the system tries to automatically reconfigure the network devices with the use of their Application Programming Interface (API) [12]. Although risk analysis involving threats, attacks or supervised networks was out of the scope of the NECOMA project, we find this project to be very interesting because the idea of an advanced network traffic analysis may be relied upon to evaluate various risks.

The PANOPTESEC [13] project was pursued by a consortium comprising Institut Mines-Télécom (France), RHEA System (Belgium), Technische Universität Hamburg-Harburg (Germany), Universität zu Lübeck (Germany), Nokia Bell Labs France (France), L'École Supérieure d'Électricité (France), ACEA (Italy), Universita degli Studi di Roma La Sapienza (Italy), Epistematica (Italy), L'Institut national de recherche en informatique et en automatique (Inria) (France), RHEA System (Netherlands) and RHEATECH (Great Britain). The outcome of the PANOPTESEC project was a system that can predict paths of cyber-attacks on the supervised IT infrastructure. To achieve this, the system must be filled with all information about the network infrastructure, including: devices, network connections between them, firewall rule sets, operating system version, application version, and so on. Having this knowledge and information about vulnerabilities in hardware and software, the system can simulate paths of attacks or malware infections. To make this simulation more actionable, it is supplemented with information about mission impact in the case of a failure of some devices [14]. Mission impact and risk analysis must be performed by the system user (e.g. organization or company) in advance [15]. These simulations and the potential mission impact are visualized alongside with examples of mitigation, to help the user take the proper action [16]. All these features make PANOPTESEC a very promising solution in terms of analyzing the risk of IT-related threats. Unfortunately, processing this amount of data requires lots of computing power. Benchmarks performed by PANOPTESEC authors show that the analysis of connections between 10,000 network nodes may take up to 1 hour [17].

WISER [18] was a project led by Atos Spain, with other participating entities including the following: Trust-It Services Limited (Great Britain), Stiftelsen Sintef (Norway), XLAB Razvoj Programske Opreme In Svetovanje (Slovenia), Aon UK Limited (Great Britain), Rexel Dévéloppement (France), Domotecnica (Italy), Enervalis (Belgium) and Aon Insurance & Reinsurance Brokers (Italy). The product of this project is now available commercially and is known as the CYBERWISER service [19]. The WISER system requires two types of input to operate. The first type of input comes from sensors (software- and hardware-based) which analyze network traffic and system logs to detect cyber-attacks. The other type of input originates from a risk analysis performed for various cyber-attack scenarios (such as denial of service attack, bypass login by brute force or DNS login attack, compromise security via trojan-malware, SQL injection, buffer overflow, relative path traversal, and so on) [20]. The risk analysis is carried out using CORAS diagrams to identify attack scenarios with the affected assets, and DEXi or R language to define Bayesian networks to model specific risks. With risk-related information obtained from sensors, the system may dynamically present the current level of threat [21]. WISER presents an interesting approach to connecting, in real time, risk analysis to specific vulnerabilities and threats.

PROTECTIVE [22] is an ongoing project of Athlone Institute of Technology (Ireland), Synyo (Austria), Poznań Supercomputing and Networking Center (Poland), The Email Laundry (Ireland), Technische Universität Darmstadt (Germany), Agency Arniec – RoEduNet (Romania), GMV Soluciones Globales Internet (Spain), Cesnet (Czech Republic), ITTI (Poland) and University of Oxford (Great Britain). As the project will conclude by September 2019, its final implementation date is subject to change. This project is focused on sharing threat intelligence between the platform's participants. At the time when this paper is being compiled, architecture of the PROTECTIVE system assumes that each participant is collecting information about network traffic within their organization, using a set of probes (software and hardware) [23]. The collected data is standardized and analyzed to identify malicious or undesired activities, or potentially unwanted applications. Based on these findings, the system creates IoCs. IoCs may then be shared with other participants to help them protect their networks or identify and mitigate attacks [24]. The description of the PROTECTIVE project contains references to risk analysis performed with regard to the participants' assets, but it lacks any details.

Summary

Over the past five years, at least four big international projects focused on cyber threats and/or risk analysis have been pursued. All projects presented above propose certain interesting ideas in the field of risk analysis, information aggregation, sharing of intelligence data, as well as monitoring and mitigating threat. Nevertheless, none of them are capable of monitoring the threat level nationwide. This shows how complex the task of analyzing risk and monitoring threats affecting the networks of organizations and enterprises of various sizes, organizational structures, IT infrastructures, etc. is. The National Cybersecurity Platform is designed to solve this problem and help enhance the level of cybersecurity.

3. Approach to the Model of Relationships between Services and Risk Assessment

One of the main motivations of the National Cybersecurity Platform is the implementation of the Directive on security of network and information systems (NIS Directive, [25]) which was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The NCP platform creates a map of key services that depend on ICT infrastructure. It is the task of the platform to achieve several objectives, such as monitoring the security of cyberspace, early detection of threats and taking proactive measures to mitigate the risks.

The risk level will be estimated for individual services, sectors and the entire cyberspace of a given country based on the vulnerabilities identified, sightings, incidents, assessment of the criticality of services and based on the criticality of relationships between individual services. Both static and dynamic risks will be analyzed. Based on the risk analysis performed in the context of services, sectors and cyberspace of the Republic of Poland, recommendations for platform participants will be issued using the expert module.

Relationships between services are presented by means of a graph depicting their mutual interdependencies, in particular as far as the aspect of security (confidentiality, integrity and availability) us concerned. The said graph presents also the affiliation of specific services to institutions (operators) and sectors. The graph depicting the relationships between key services is based on data from questionnaires completed by the platform's clients.

4. Information Used to Build Situational Awareness

The following types of information may be relied upon to analyze and calculate risk:

- vulnerabilities,
- Indicators of Compromise (IoC),
- sightings,
- incidents,
- network monitoring results (e.g. results of open port scanning),
- inventory (software and hardware used, relationships with services and criticality of relationships),
- catalog of services and relationships between services.

The most important types of information are described in the following subsections.

4.1. Vulnerabilities

One may undoubtedly argue that each software and hardware component suffers from certain vulnerabilities, even if many of them have failed to be discovered so far. However, the claim that each software element is equally sensitive is not true and unjustified. The normal process of revealing a newly discovered vulnerability assumes that the vendor of the product in which the vulnerability has been discovered is informed first. The vendor, after conducting an investigation and relevant research, prepares an appropriate software patch (also known as a fix or an update) which should eliminate the vulnerability concerned. After preparing the patch, the vendor informs (for example via bulletins published on the vendor's website) all potential users and the community about the new fix and about the vulnerability itself. This process is known as the process of responsible disclosure. Vulnerabilities are discovered not only by white hats (cyber security analysts whose goal is to boost the level of the software security), but also by black hats (crackers whose purpose is to compromise information systems to obtain certain information or to prevent their fair use). When the cracker finds a new vulnerability (so called "0-day"), they try to exploit it to generate benefits, instead of informing the vendor. Therefore, unknown vulnerabilities are associated with an enormous potential to compromise system security [1].

The vulnerability management system should support the system administrator in two areas. First of all, its main task should be to support the administrator in the process of managing updates. The system administrator should be able to indicate all software components making up the system. Vulnerabilities and patches published after the last update should be detected using an automated system that collects information about patches and vulnerabilities obtained from several different sources. Secondly, the vulnerability management system should assess the technical risks associated with the software used. This risk stems from the existing security vulnerabilities [1].

Technical vulnerability databases are very important, but they contain information about well-known vulnerabilities only (mainly those for which patches have been released). To calculate risk, the administrator has to identify the presence of a vulnerable asset, and, consequently, the presence of the vulnerability itself. Because of that, in theory, the chances that the administrator takes corrective actions are greater than the chances that the administrator conducts (even in an automated manner) a risk analysis taking into account the vulnerability concerned. After successful correction, no additional risk associated with this vulnerability is present (due to its elimination). In practice, however, sometimes it is not possible to apply the patch or other proposed recommendations or such measures cannot be introduced immediately. In such scenario, it makes sense to update the risk calculations performed.

To calculate the level of risk affecting a system or a service based on its vulnerabilities, the Common Vulnerability Scoring System (CVSS) may be used. CVSS is a methodology that characterizes the impact of security vulnerabilities. The CVSS score may be perceived as an indicator of the severity of a specific vulnerability. The CVSS score may vary from 0.0 to 10.0, where values from 0.0 to 3.9 indicate a “low” level of severity, and values from 7.0 to 10.0 mean “high” or “critical” severity. The CVSS result is widely used as an indicator of the severity of vulnerabilities, but not all sources of information list it [1].

Risk calculation will be performed by each client based on the vulnerability database shared by the operational center. Each client should perform inventory identification, and based thereon, they should automatically match vulnerabilities that may affect their systems and services.

Many approaches rely on NVD only, as the best-known database of security vulnerabilities. However, NVD is not the only database and it does not provide the most information. Several limitations of the NVD database were also indicated by the author of [26]. While conducting our research, we analyzed the generally available databases of vulnerabilities and patches. One may conclude that in order to build a comprehensive database of vulnerabilities, many sources of information about vulnerabilities should be relied upon.

4.2. Inventory

The inventory, which can be perceived as a database of IT assets, is crucial from the point of view of the vulnerability management process. The inventory needs to be taken by each client individually. However, details of the inventory are not shared with the operations center or any other client. Lists of software or hardware elements and applications are used to calculate the risks which stem from the existing vulnerabilities.

4.3. Indicators of Compromise and Sightings

Indicators of compromise are characteristics observed within a network or a system indicating an intrusion. Aggregation and provision of such information to clients may be beneficial for security monitoring. The presence of an artifact described by IoC (sighting) may also impact current risk calculations.

4.4. Incidents

Incidents reported by all participants of the platform may be aggregated by the operations center and may be used for risk assessment purposes. Based on historical information, the incident prediction mechanisms may be implemented. Information about incidents reported by various institutions may be used to identify similar features of incidents and targeted institutions. Based thereon, the risk of the threat propagating between services and institutions may be estimated as well.

5. Risk Calculation

One of the main goals of the National Cybersecurity Platform is to provide a comprehensive analysis of risks arising from the potential exploitation of known vulnerabilities affecting the company’s IT assets, as well as from potential security incidents, such as: hacker attacks, malware infections or data breaches. The risk analysis process is divided between clients and the NCP operations center, because the results of this analysis concern risks at the institution- and nationwide level. The flow of data (related to risk analysis) between the client and the NCP operations center is depicted in Fig. 1. More details on risk analysis may be found in the subsequent sections.

5.1. Institution Level

Risk analysis performed at the institution level concerns cyberthreats to the company’s IT infrastructure that supports the services. The risk analysis is carried out for each service offered by the client. The National Cybersecurity Platform is responsible for services which are essential for the country’s economy or security. The criteria for such services are set out in the National Cybersecurity System Act. The services may produce goods or may be completely intangible. For the purpose of a more detailed risk analysis, it is important to define whether the risk analysis cover intangible services rendered in an electronic form (the so called e-service) or not.

Each client joining NCP has to fill out a questionnaire about the services they would like the National Cybersecurity Platform to cover (denoted as S_E). The questions are related to the following information: type of service (electronic or not), scale of service expressed in applicable units of measure (e.g. tons of coal for mines or number of passengers in the case of transport services) – (global criticality of the service – $C_g^{S_E}$), relevance of service for the client’s business (internal criticality of $C_i^{S_E}$ service), standards, procedures and means of security incorporated to protect the service against cyberthreats and the time needed to recover the service after a failure (the shortest and the longest period of time experienced before the questionnaire is filled out).

There are also questions about relationships between services enrolled in NCP and supporting services provided by a third party. The questionnaire examines the strength of the relationship between such services. The client has to declare the portion of their enrolled services that depends on each supporting service (denoted as S_S), as far as their confidentiality, integrity and availability are concerned. The strength of the relationship $K^{(S_S \to S_E)}$ is defined as a 3×3 matrix with a numerical value for each pair of one of the three aspects. For example, in the context of the relationship between integrity and availability, this value indicates the impact of the integrity of the supporting service being compromised on the availability of the enrolled service. Such a relationship may be observed, for example, if one service aggregates data from other services

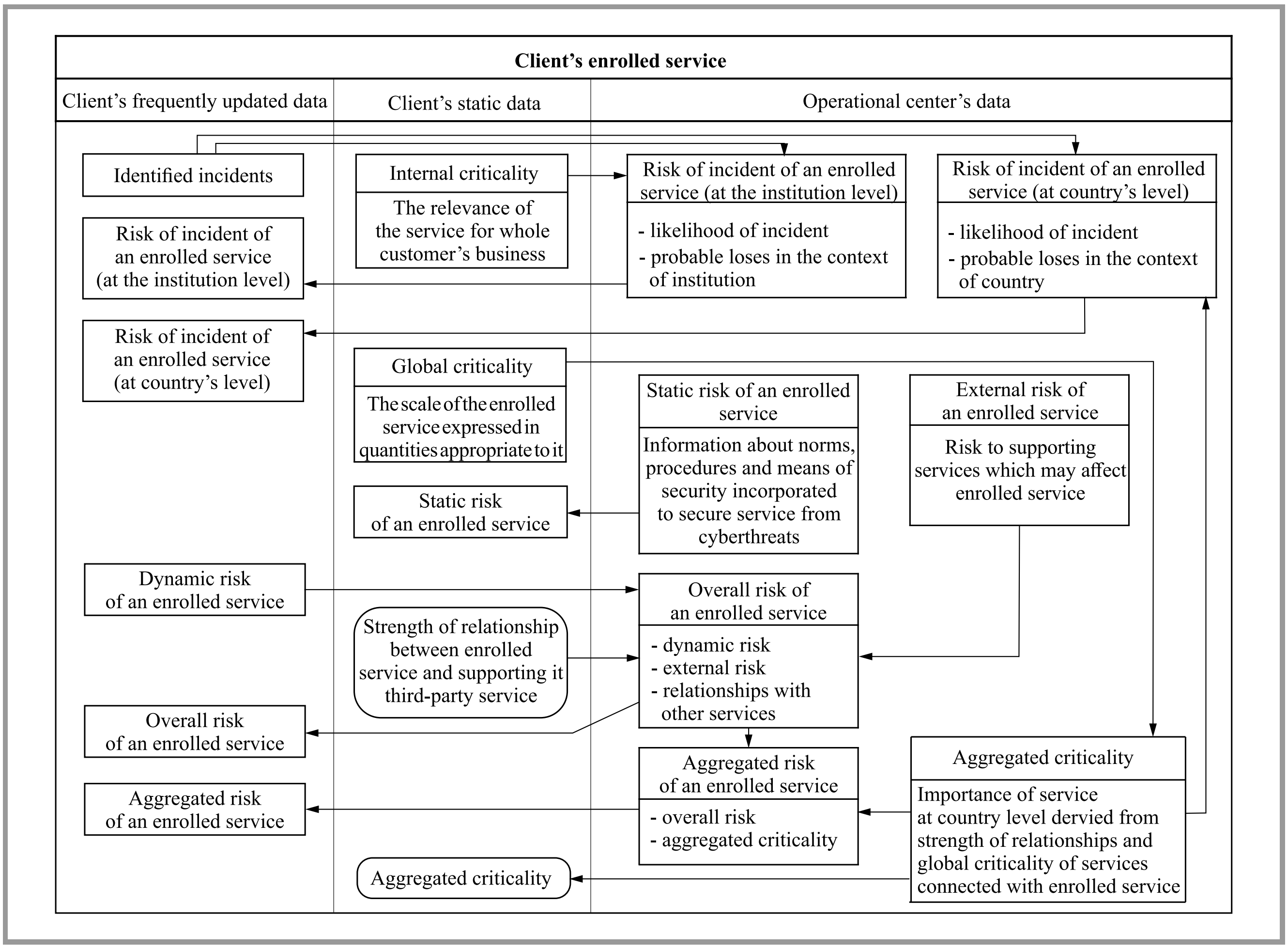
Client's enrolled service
Client's frequently updated data
Client's static data
Operational center's data
Identified incidents
Internal criticality
The relevance of the service for whole customer's business
Risk of incident of an enrolled service (at the institution level)
- likelihood of incident
- probable loses in the context of institution
Risk of incident of an enrolled service (at country's level)
- likelihood of incident
- probable loses in the context of country
Risk of incident of an enrolled service (at the institution level)
Risk of incident of an enrolled service (at country's level)
Global criticality
The scale of the enrolled service expressed in quantities appropriate to it
Static risk of an enrolled service
Information about norms, procedures and means of security incorporated to secure service from cyberthreats
External risk of an enrolled service
Risk to supporting services which may affect enrolled service
Static risk of an enrolled service
Dynamic risk of an enrolled service
Overall risk of an enrolled service
- dynamic risk
- external risk
- relationships with other services
Strength of relationship between enrolled service and supporting it third-party service
Overall risk of an enrolled service
Aggregated risk of an enrolled service
- overall risk
- aggregated criticality
Aggregated criticality
Importance of service at country level dervied from strength of relationships and global criticality of services connected with enrolled service
Aggregated risk of an enrolled service
Aggregated criticality

Fig. 1. Data flow between client and National Cybersecurity Platform's operations center.

to return some complex datasets. If one of the data pools loses its integrity, no access to the output dataset should be provided, as it may be based on invalid or missing data. If no such a relationship for a certain pair of aspects exists, the value in the matrix equals zero. The pairs of attributes whose consideration is mandatory are presented in Table 1.

Table 1
Strength of relationship matrices $K^{(S_S \to S_E)}$. Depending on the character of the connected services – enrolled and supporting service – different sets of pairs of aspects are mandatory to be considered by the client (marked with ✓)

		Supporting e-service			Supporting service		
		C	I	A	C	I	A
Enrolled e-service	C	✓	✓	✓	X	X	✓
	I	✓	✓	✓	X	X	✓
	A	✓	✓	✓	X	X	✓
Enrolled service	C	X	X	X	X	X	X
	I	X	X	X	X	X	X
	A	✓	✓	✓	X	X	✓

Moreover, the client has to declare how long his service is capable of running after a failure of one of the supporting services.

All information referred to above may be updated on a regular basis, for instance every six months or once a year, as well as when the client makes any changes to their organization that affect the previously stated answers. Such data are referred to as static. Information about the standards, procedures and means of security incorporated to protect the service against cyberthreats is used to calculate the static risk affecting the enrolled service – $R_{is}^{S_E}$. These calculations are performed by the NCP operations center.

Some information needs to be updated frequently. Clients will be receiving a definition of new vulnerabilities discovered in the software and hardware as soon as the NCP's operations center becomes aware of them. It is the client's responsibility to check if their IT infrastructure is prone to these vulnerabilities, and if so, the client has to update the dynamic risk indicator relevant for the enrolled service – $R_{id}^{S_E}$ as quick as possible and return the result to the NCP operations center. To calculate the dynamic risk value pertaining to a given service, the client has to follow instructions provided by National Cybersecurity Platform or use their own risk calculation method, provided it takes into account the IT infrastructure and the presence of vulnerabilities. Dynamic risks may be valuable to the NCP client as they may identify IT assets that require extra attention in terms of cybersecurity and potential losses that may be suffered in the event of a compromise, with the context of the services supported by these assets taken into consideration. The client's reports on incidents detected in their infrastructure also constitute information that is important from the point of view of risk analysis. These incidents may be related to malware, cyberattacks, data security breaches or any other cyber threats that may interrupt or completely stop a given service. To help clients detect incidents, the NCP operations center will provide them with indicators of compromise (IoC) for known cyber threats. Knowledge about the number and severity of incidents detected by clients is used to calculate the risk of an incident affecting the service, in the context of the institution – $R_{iI}^{S_E}$ and the risk of an incident affecting the service in the context of the entire country – $R_{cI}^{S_E}$. These calculations are carried by the operations center.

5.2. Operations Center Level

The National Cybersecurity Platform's operations center collects dynamic risk values for all enrolled services. The knowledge of such values, as well as of details concerning relationships between services (reported by clients in questionnaires), the software used by the operations center is capable of calculating how the risk of one service affects the risk of associated services (the ones depending on the former service). This type of risk is referred to as external risk of the enrolled service – $R_e^{S_E}$. In conjunction with dynamic risk, external risk determines the overall risk affecting the enrolled service – $R_o^{S_E}$. These risks may help clients perceive their business in the context of a network of services.

Knowing the overall risk affecting the services and the importance of those services for the country's economy and for the continuity of other businesses, the NCP operations center may calculate the aggregated of all enrolled services – $R_a^{S_E}$. As this risk takes into account the importance of services at the national level ($C_a^{S_E}$), it helps analysts at the NCP operations center monitor the current level of risk of the vulnerabilities known to be existing in supervised services of being exploited. The aggregated risk of services is utilized to calculate the risk for economic sectors, groups of services or for the entire cyberspace. This will be elaborated on in the following section.

Analysts at the operations center will have access to statistics and data from sources other than the clients only. Such additional information will be presented on a per service basis, with the ability to aggregate it for a specific set of services (e.g. the entire cyberspace, an economic sector, etc.) in order to provide a quick security overview. Statistical data may be presented as trends, total and averages for a period of time defined by an analyst. Such statistics includes the following: number of incidents along with their severity, number of detected vulnerabilities and number of mitigated vulnerabilities. The system will also show an indicator related to ongoing cyber-attacks affecting specific services. Additional data from auxiliary sources includes events from the n6 database [9] and the results of automatic scans of hosts visible in the Internet. This information will be presented on a per-service or per-client basis, depending on how detailed the information about IP address space the client provides to NCP is.

5.3. Risk Propagation

As mentioned above, the NCP operations center will be able to calculate how the risk affecting one service may impact the risks pertaining to another service. Risk propagation may be monitored thanks to detailed information about the relationships between services. The idea of risk propagation is presented in Fig. 2. Each client has to describe the strength of the connection between their services and the support provided by third party services. Such an approach offers the most reliable data, as business owners have the best knowledge on the degree to which their services rely on others. Information about the connection may be very detailed, as it may describe how the fact of any aspect (confidentiality, integrity and availability) of the support service being compromised may impact any aspect of the enrolled service – up to 9 separate values of influence are distinguished (see Table 1).

The level of reliability of information about the relationships between services is a major but not the only problem experienced when monitoring risk propagation. The other problem consists in finding a solution to cyclic relationships between services. It is possible that one service relies on another which, in turn, depends on the first one – this creates a loop in the graph of relationships between services. In such a loop, the increase in the dynamic risk affecting one of the services will boost the overall risk as well. A higher overall risk will cause a higher external risk affecting the dependent service. This will lead to a growth in the overall risk of the dependent service (as overall risk is a combination of dynamic risk and external risk). This increase in the risk of one of the services would propagate infinitely over all services in the loop.

Software relied upon by the National Cybersecurity Platform uses a proprietary algorithm to propagate changes to risk values between services connected within loops, preventing such an infinite growth or reduction of risk due to propagation. This makes the results of risk analysis more realistic, as they take into account the fact the compromising of one of the services may propagate even to services which are not directly related.

5.4. High-level Situational Cybersecurity Awareness

One of the advantages of the National Cybersecurity Platform is the ability to aggregate the risks of a set of services. It helps analysts at the operations center to assess the security in cyberspace. An analyst may quickly check the risk

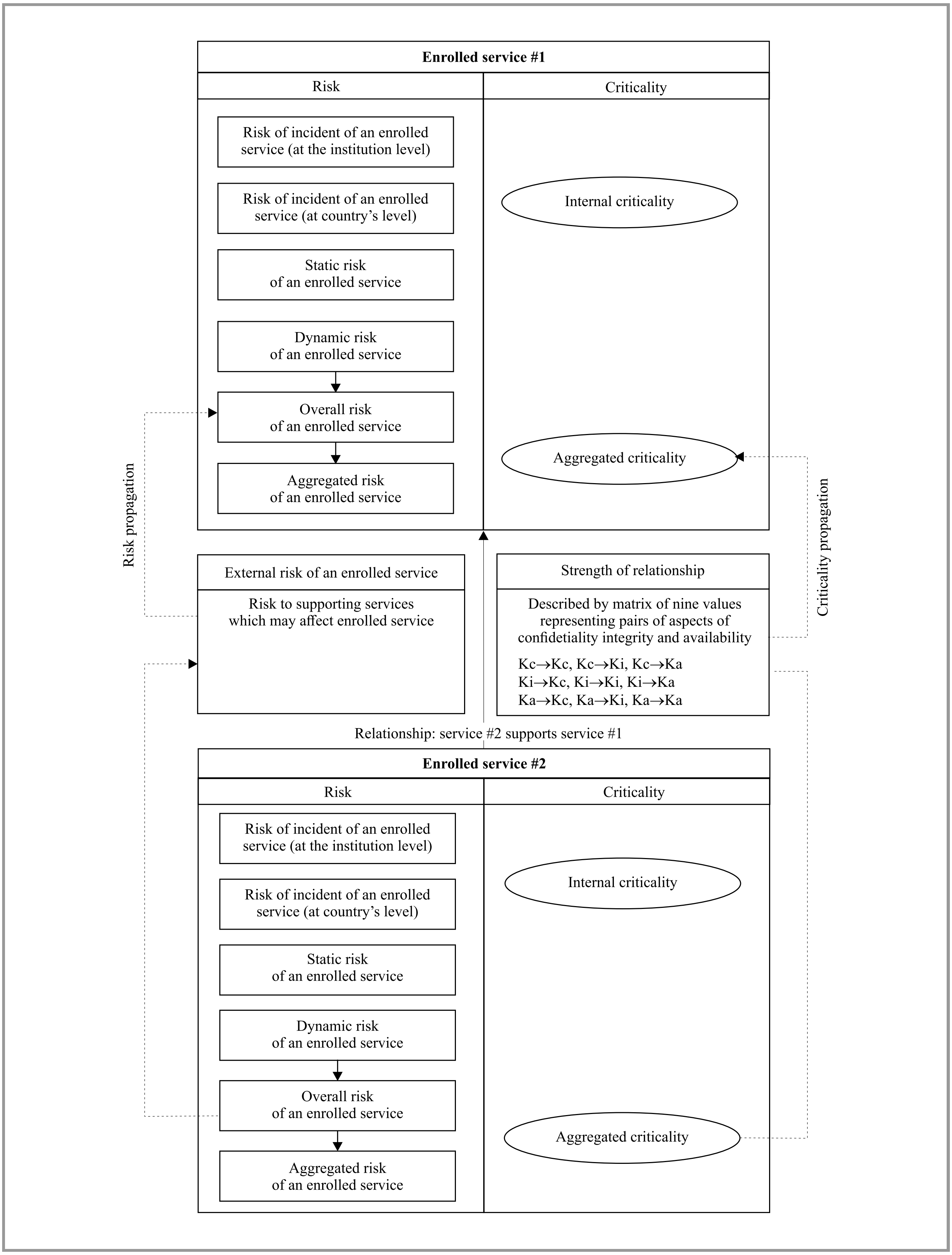
Enrolled service #1
Risk
Criticality
Risk of incident of an enrolled service (at the institution level)
Risk of incident of an enrolled service (at country's level)
Static risk of an enrolled service
Dynamic risk of an enrolled service
Overall risk of an enrolled service
Aggregated risk of an enrolled service
Internal criticality
Aggregated criticality
Risk propagation
Criticality propagation
External risk of an enrolled service
Risk to supporting services which may affect enrolled service
Strength of relationship
Described by matrix of nine values representing pairs of aspects of confidetiality integrity and availability
Kc→Kc, Kc→Ki, Kc→Ka
Ki→Kc, Ki→Ki, Ki→Ka
Ka→Kc, Ka→Ki, Ka→Ka
Relationship: service #2 supports service #1
Enrolled service #2
Risk
Criticality
Risk of incident of an enrolled service (at the institution level)
Risk of incident of an enrolled service (at country's level)
Static risk of an enrolled service
Dynamic risk of an enrolled service
Overall risk of an enrolled service
Aggregated risk of an enrolled service
Internal criticality
Aggregated criticality

Fig. 2. Risk propagation diagram.

values for the entire cyberspace, for each economic sector or for any set of services.

Aggregation may also show some emerging threats affecting services in cyberspace. For example, analysts can easily spot if the overall risk is rising in a given economic sector. Such a situation may indicate that there is a new vulnerability of some element of the IT infrastructure (software or hardware) which is popular among services in the sector concerned.

In addition to risk aggregation, NCP will enable aggregating other information, such as reported incidents or data from external sources, as described above. For example, it may be helpful in identifying if cyber-attacks are aimed at a particular type of services or a specific industry, as it will identify the service for which the incident has been reported over the past few weeks.

Such a detailed insight into the level of risks experienced so far, as well as into incident reports, sightings and other security-related data, helps both analysts at the operations center and NCP clients manage their risk and keep the essential services safe from cyberthreats.

6. Summary and Future Work

To the best of the authors' knowledge, the approach proposed is the first which may be applied at the national level. The novelty of the approach is based on real-time risk analysis performed by clients at various levels. Because of a unified and quantitative methodology is used, the results may be aggregated on the national level. Based on the risk calculation approach proposed, one may foresee threats and build situational awareness by monitoring the current situation. The proposed approach requires further research and verification in the operational environment, but it seems to be rather promising.

Acknowledgements

Work done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre of Research and Development in the frame of CyberSecIdent Programme.

References

[1] M. Janiszewski, A. Felkner, and J. Olszak, "Trust and risk assessment model of popular software based on known vulnerabilities", *Int. J. of Electron. and Telecommun.*, vol. 63, pp. 329–336, 2017 (doi: 10.1515/eletel-2017-0044).

[2] IBM OpenPages with Watson [Online]. Available: https://www.ibm.com/us-en/marketplace/governance-risk-and-compliance (accessed 23.11.2018).

[3] Data Center Management and Network Management Software from Device42 Software [Online]. Available: https://www.device42.com/ (accessed 23.11.2018).

[4] Helix Discovery – BMC Software [Online]. Available: https://www.bmc.com/it-solutions/discovery-dependency-mapping.html (accessed 23.11.2018).

[5] Asset Inventory [Online]. Available: https://www.qualys.com/apps/asset-inventory/ (accessed 23.11.2018).

[6] Integrated Risk Management [Online]. Available: https://www.rsa.com/en-us/products/integrated-risk-management (accessed 23.11.2018).

[7] Products by Category – ServiceNow [Online]. Available: https://www.servicenow.com/products-by-category.html (accessed 23.11.2018).

[8] NECOMA [Online]. Available: http://www.necoma-project.eu/ (accessed 26.11.2018).

[9] n6 – network security incident exchange [Online]. Available: https://n6.cert.pl/ (accessed 26.11.2018).

[10] PhishTank [Online]. Available: https://www.phishtank.com (accessed 26.11.2018).

[11] NECOMA Nippon-European Cyberdefense-Oriented Multilayer threat Analysis "Deliverable D1.4: Threat Data Final Report" April 20th, 2016 [Online]. Available: http://www.necoma-project.eu/m/filer_public/55/ec/55ec2e53-14fa-40f4-a67f-c7a092cfe463/necoma-d14.pdf (accessed 26.11.2018).

[12] NECOMA Nippon-European Cyberdefense-Oriented Multilayer threat Analysis "Deliverable D3.1: Policy Enforcement Point Survey" November 30th, 2013 [Online]. Available: http://www.necoma-project.eu/m/filer_public/0e/75/0e75c773-a857-416b-99a0-090ec0b38388/necoma-d31r207.pdf (accessed 26.11.2018).

[13] PANOPTESEC [Online]. Available: http://www.panoptesec.eu (accessed 26.11.2018).

[14] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D3.1.2: System High Level Design" March 27th, 2015 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D312_v2.0-QA-Approved.pdf (accessed 26.11.2018).

[15] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D5.1.1 – Response System for Dynamic Risk Management Requirements" March 27th, 2015 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D511_v2.1-QA-Approved.pdf (accessed 26.11.2018).

[16] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D6.3.2: Visualization Integration Prototype Report" June 30th, 2016 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D632_v1.0-QA-Approved.pdf (accessed 26.11.2018).

[17] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D7.4.2 Demonstration System Prototype Report" November 5th, 2016 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D742_v1.1.pdf (accessed 26.11.2018).

[18] Deliverables [Online]. Available: https://cyberwiser.eu/deliverables (accessed 26.11.2018).

[19] CYBERWISER.eu – Cyber Range & Capacity Building in Cybersecurity [Online]. Available: https://www.cyberwiser.eu (accessed 26.11.2018).

[20] Wide – Impact cyber Security Risk framework "D3.1 – Cyber Risk Patterns" May 31st, 2016 [Online]. Available: https://cyberwiser.eu/system/files/WISER_D3_1_v10_0.pdf (accessed 26.11.2018).

[21] Wide – Impact cyber Security Risk framework "D3.4 Cyber Risk Modelling Language and Guidelines, Final Version" March 29th, 2017 [Online]. Available: https://cyberwiser.eu/system/files/WISER_D3_4_v10_0.pdf (accessed 26.11.2018).

[22] Protective – Proactive Risk Management through Improved Cyber Situational Awareness [Online]. Available: https://protective-h2020.eu (accessed 26.11.2018).

[23] PROTECTIVE Proactive Risk Management through Improved Cyber Situational Awareness "D6.1 Framework Specification" June 28th, 2017 [Online]. Available: https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D6.1-E-0417-Framework-Specification.pdf

[24] PROTECTIVE Proactive Risk Management through Improved Cyber Situational Awareness "D2.1 Requirements Capture, Specification, Architectural Design and Model" June 15th, 2017 [Online]. Available: https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D2.1-E-0615-Requirements_Architecture.pdf (accessed 26.11.2018).

[25] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union" [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1

[26] A. Felkner, "Przegląd i analiza źródeł informacji o podatnościach (Review and analysis of sources of information about vulnerabilities)", *Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne*, vol. 8-9/2016, 2016, pp. 929–933 (doi: 10.15199/59.2016.8-9.37) [in Polish].

Marek Janiszewski is a Research Associate on the Information Security Methods Team in the R&D division at Research and Academic Computer Network NASK. His research interests include intrusion detection systems, penetration testing, personal data and identity management and trust and reputation management systems. He is preparing his Ph.D. thesis at the Telecommunication Institute, Warsaw University of Technology.

https://orcid.org/0000-0001-8965-6302
E-mail: marek.janiszewski@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Anna Felkner holds a Ph.D. degree in Information Technology from the Warsaw University of Technology and an M.Sc. degree from Bialystok University of Technology. She is an Assistant Professor and head of the Information Security Methods Team. Her interests include access control, trust modeling, risk analysis and vulnerability management. She is the author of over forty publications, has spoken at many conferences.

https://orcid.org/0000-0003-3813-4840
E-mail: anna.felkner@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Piotr Lewandowski is a specialist on the Information Security Methods Team in the R&D division at Research and Academic Computer Network NASK. His research interests include practical aspects of personal and enterprise networks' security. He received an M.Sc. in Physics from the Warsaw University of Technology.

https://orcid.org/0000-0003-0964-6812
E-mail: piotr.lewandowski@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland